

УДК 336.225:004.056(575.2)
JEL: M48; O16

<https://doi.org/10.33619/2414-2948/131/49>

**ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СФЕРЕ
НАЛОГОВОГО АДМИНИСТРИРОВАНИЯ: ЭМПИРИЧЕСКИЙ АНАЛИЗ
ОБЩЕСТВЕННОГО ВОСПРИЯТИЯ И ИНСТИТУЦИОНАЛЬНОГО ДОВЕРИЯ
В КЫРГЫЗСКОЙ РЕСПУБЛИКЕ**

©Эргешова А. Р., Кыргызский национальный университет
им. Ж. Баласагына, г. Бишкек, Кыргызстан, ainuraergeshova@gmail.com
©Орозмаматова Д. А., ORCID: 0009-0001-1027-4801, Университет Ритсумейкан,
г. Киото, Япония

**INFORMATION SECURITY IN TAX ADMINISTRATION: AN EMPIRICAL ANALYSIS
OF PUBLIC PERCEPTION AND INSTITUTIONAL TRUST IN THE KYRGYZ REPUBLIC**

©Ergeshova A., Kyrgyz National University
named after Zh. Balasagyn, Bishkek, Kyrgyzstan, ainuraergeshova@gmail.com
©Orozmamatova D., ORCID: 0009-0001-1027-4801, Ritsumeikan University, Kyoto, Japan

Аннотация. Ускоренная цифровая трансформация фискального сектора в развивающихся экономиках создала фундаментальное институциональное противоречие: масштабирование обязательного электронного администрирования опережает рост общественного доверия к системам защиты фискальных данных. В настоящей статье на основе эмпирического анализа опроса 409 респондентов и тематической кластеризации 307 открытых ответов исследуется структура запроса граждан Кыргызской Республики на обеспечение кибербезопасности в налоговой сфере. Метод контент-анализа и кластеризации позволил выявить восемь ключевых векторов восприятия цифровых рисков. Результаты демонстрируют преобладание запроса на комплексное государственное администрирование (38,1%) и репрессивно-правовое регулирование (19,5%), тогда как сугубо технические решения (шифрование, многофакторная аутентификация) воспринимаются лишь как сопутствующий инструмент (18,6%). Авторы доказывают наличие парадокса институционального доверия: обязательная интеграция налогоплательщиков в цифровые платформы (включая систему «Түндүк») воспринимается обществом не только через призму защиты от внешних кибератак, но и как источник потенциальной утечки данных из-за фактора внутренних уязвимостей. Сделан вывод, что дальнейшая цифровизация фискального администрирования без параллельного укрепления институтов правовой ответственности и независимого аудита рискует вызвать латентное сопротивление налогоплательщиков, отток капитала и сжатие налогооблагаемой базы. Полученные результаты расширяют научную дискуссию о соотношении цифрового контроля, гибридных киберугроз и доверия к институтам власти в странах с переходной экономикой.

Abstract. Accelerated digital transformation of the fiscal sector in emerging economies has generated a fundamental institutional tension: the scaling of mandatory electronic administration outpaces the growth of public trust in fiscal data protection systems. Based on an empirical survey of 409 respondents and thematic clustering of 307 open-ended responses, this paper examines the structure of public demand for cybersecurity in the tax domain of the Kyrgyz Republic. A content analysis and thematic clustering methodology revealed eight primary vectors of public risk perception. The findings demonstrate a predominant demand for comprehensive state governance (38.1%) and punitive legal enforcement (19.5%), whereas purely technical solutions (encryption, authentication) are perceived only as a supporting instrument (18.6%). The authors prove the existence of an institutional trust paradox: mandatory integration of taxpayers into digital platforms (including the "Tunduk" system) is perceived by society not only through the prism of protection from external cyberattacks, but also as a source of potential data leakage due to the factor of internal vulnerabilities. A conclusion is drawn that further digitalization of fiscal administration without parallel strengthening of institutions of legal responsibility and independent audit risks causing latent resistance of taxpayers, capital outflow and squeezing of the tax base. The results expand the scientific discussion on the relationship of digital control, hybrid cyber threats and trust in institutions of power in transition economies.

multi-factor authentication) are viewed merely as secondary instruments (18.6%). The authors argue for the existence of an institutional trust paradox: the mandatory integration of taxpayers into digital platforms (including the "Tunduk" system) is perceived by the public not only through the lens of external cyber threat mitigation but also as a point of vulnerability to internal data leaks. The study concludes that further digitalization of tax administration without parallel strengthening of legal accountability mechanisms and independent auditing risks triggering latent taxpayer resistance, capital flight, and contraction of the tax base. These results contribute to the academic debate on the interplay between digital surveillance, hybrid cyber threats, and institutional trust in transition economies.

Ключевые слова: кибербезопасность; налоговое администрирование; цифровизация фискальной сферы; институциональное доверие; киберриски; инвестиционный климат; Кыргызская Республика; система «Тундук».

Keywords: cybersecurity governance; tax administration; fiscal digitalization; institutional trust; cyber risks; investment climate; Kyrgyz Republic; Tunduk system.

Цифровизация налогового администрирования в Кыргызской Республике кардинально трансформирует характер взаимодействия между государством и частным сектором. Внедрение электронных сервисов, хотя и повышает прозрачность процессов, одновременно формирует новую категорию институциональных рисков. В современных условиях устойчивость национальной экономики определяется не только уровнем фискальной нагрузки, но и способностью государственных институтов гарантировать сохранность чувствительных цифровых активов граждан и бизнеса. Актуальность исследования обусловлена необходимостью эмпирической оценки эластичности предпринимательской активности по отношению к киберрискам. Цель работы — определить структуру общественного запроса на обеспечение безопасности фискальных данных в Кыргызской Республике и оценить потенциальное влияние кибератак на инвестиционную привлекательность страны [1-4].

Теоретический фундамент исследования опирается на положения институциональной экономики и концептуальные модели экономики кибербезопасности. Взаимосвязь между жесткостью фискального администрирования, уровнем защищенности информационного контура госструктур и готовностью экономически активных агентов к добровольному соблюдению налоговой дисциплины анализируется сквозь призму институционального доверия. Сбор первичного эмпирического материала проводился посредством анонимного социологического онлайн-опроса на базе платформы Google Forms. Выборка объединяет 409 респондентов в возрасте от 18 до 75 лет, представляющих ключевые группы экономически активного населения Кыргызской Республики: субъектов малого, среднего и крупного бизнеса, наемных работников, профильных IT-специалистов и экспертов финансово-банковского сектора (<https://sti.gov.kg/>).

Конструкция эмпирического инструментария построена на триангуляции количественных и качественных методов анализа. *Количественный модуль:* нацелен на измерение поведенческих установок хозяйствующих субъектов при наступлении кризисных ситуаций в цифровом контуре. В частности, ключевым индикатором доверия выступила оценка готовности продолжать предпринимательскую деятельность при компрометации реестров ГНС. В качестве сопутствующих факторов анализировалось восприятие кибербезопасности как элемента инвестиционной привлекательности юрисдикции и уровень осознания рисков при трансграничном обмене фискальной информацией [1].

Качественный модуль: базируется на методе индуктивного контент-анализа и тематической кластеризации 307 открытых текстовых ответов респондентов на вопрос: «Какие меры государство должно принять, чтобы защитить данные налогоплательщиков от киберугроз?». Данный блок позволил декомпозировать глубинный запрос общества на 8 содержательных векторов реагирования.

Синтез полученных количественных данных с качественными категориями дал возможность зафиксировать текущую степень уязвимости институционального доверия к фискальным органам и количественно оценить потенциальные угрозы для налогооблагаемой базы Кыргызской Республики при компрометации цифровых реестров. Центральным индикатором институциональной устойчивости выступает готовность бизнеса сохранять присутствие в легальном поле страны при наступлении кризисных киберинцидентов. Ответы 409 респондентов на вопрос: «Если бы произошла утечка персональных данных, хранящихся в налоговой службе, стали бы вы снова вести бизнес в этой стране?» распределились следующим образом (Рисунок 1): 39,1% (160 чел.) — Затрудняюсь ответить (состояние высокой институциональной неопределенности); 36,4% (149 чел.) — Нет (категорический отказ от ведения бизнеса в стране); 22,0% (90 чел.) — Да (готовность продолжать деятельность); 2,5% (10 чел.) — респонденты, не занимающиеся бизнесом или являющиеся сотрудниками ГНС. Суммарно 75,5% респондентов (39,1% неопределившихся и 36,4% давших прямой отрицательный ответ) формируют критическую массу уязвимости.

Если бы произошла утечка персональных данных, хранящихся в налоговой службе, стали бы вы снова вести бизнес в этой стране?
409 ответов

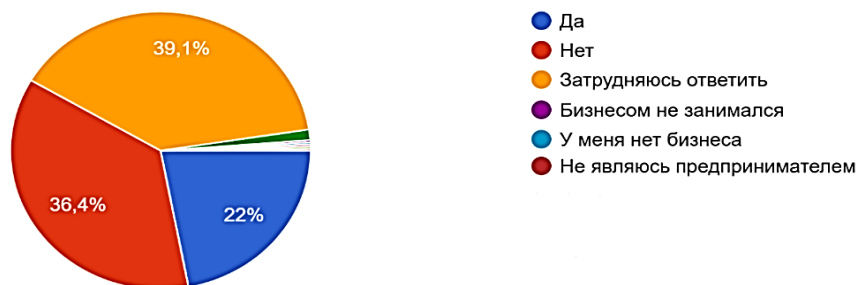


Рисунок 1. Поведенческие сценарии бизнеса при компрометации фискальных данных

С позиций финансово-экономического анализа категория «затруднившихся с ответом» (39,1%) представляет собой наиболее лабильный сегмент. При отсутствии законодательно закрепленных гарантий и компенсаций любой резонансный случай компрометации данных трансформирует этих предпринимателей в сторонников релокации капитала или перехода на наличный расчет. Группа, выбравшая вариант «Да» (22,0%), характеризуется либо высокой локальной привязкой бизнеса без возможности релокации, либо недооценкой угроз социальной инженерии и промышленного шпионажа.

Для проверки гипотезы о том, что цифровая устойчивость стала компонентом странового рейтинга, респондентам был задан вопрос: «Смотрят ли инвесторы на уровень киберзащиты страны перед вложением денег?» (Рисунок 2). 74,5% (304 чел.) — Да; 22,3% (91 чел.) — Не знаю; 3,2% (13 чел.) — Нет. Почти три четверти опрошенных демонстрируют осознание того, что понятие Digital Resilience (цифровая устойчивость) трансформировалось в ключевой критерий оценки риск-профиля юрисдикции. Инвесторы оценивают риск утечки коммерческой тайны и реестров собственников наравне со ставками налогов и судебной

защитой прав собственности. Доля затруднившихся с ответом (22,3%) указывает на сохраняющийся информационный разрыв у части малого бизнеса, воспринимающего инвестиционную привлекательность исключительно через традиционные материальные активы (земля, сырье, инфраструктура).

Смотрят ли инвесторы на уровень киберзащиты страны перед вложением денег?
408 ответов

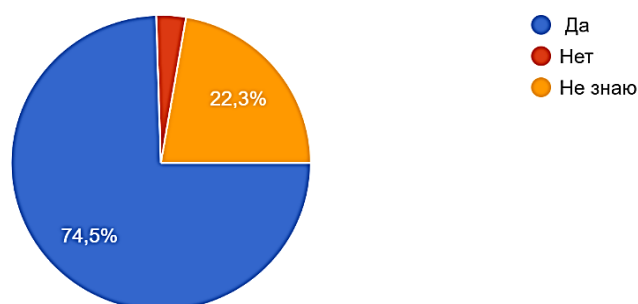


Рисунок 2. Восприятие киберзащиты как фактора инвестиционного климата

В контексте участия Кыргызской Республики в ЕАЭС и перспективах интеграции в международные системы автоматического обмена информацией (стандарты ОЭСР CRS/AEOI) особое значение приобретает безопасность межгосударственных каналов передачи данных (Рисунок 3). На вопрос: «Важна ли кибербезопасность при обмене налоговыми данными между государствами?» получены следующие результаты: 90,9% (371 чел.) — Да; 7,6% (31 чел.) — Не знаю; 1,5% (6 чел.) — Нет. Показатель в 90,9% фиксирует абсолютный общественный консенсус. Бизнес четко понимает, что передача фискальной информации по внешним контурам без применения сквозных стандартов шифрования создаёт прямую угрозу перехвата сведений иностранными конкурентами и деанонимизации логистических цепочек.

Важна ли кибербезопасность при обмене налоговыми данными между государствами?
408 ответов

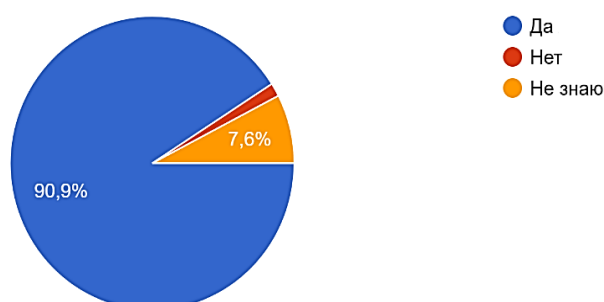


Рисунок 3. Трансграничный контекст и межгосударственный обмен данными

Для выявления глубинных установок общества в отношении необходимых государственных мер защиты данных был проведен контент-анализ 307 открытых ответов. Индуктивная тематическая кластеризация позволила распределить запросы по 8 категориям (Таблица).

Таблица

СТРУКТУРА ОТКРЫТЫХ ОТВЕТОВ РЕСПОНДЕНТОВ ПО НАПРАВЛЕНИЯМ
НЕОБХОДИМЫХ МЕР КИБЕРЗАЩИТЫ В ФИСКАЛЬНОЙ СФЕРЕ

Кластер / Направление реагирования	Доля (%)	Количество респондентов
Комплексная государственная система защиты	38.1	117
Ужесточение законодательства и ответственности	19.5	60
Технико-программное совершенствование	18.6	57
Затруднились ответить / Отсутствие позиции	16.6	51
Кадровое обеспечение и ИТ-компетенции	7.8	24
Аудит, мониторинг и проверка на уязвимости	6.2	19
Повышение цифровой и киберграмотности	3.6	11
Международный опыт и стандарты ОЭСР	2.0	6
ИТОГО	100.0	307

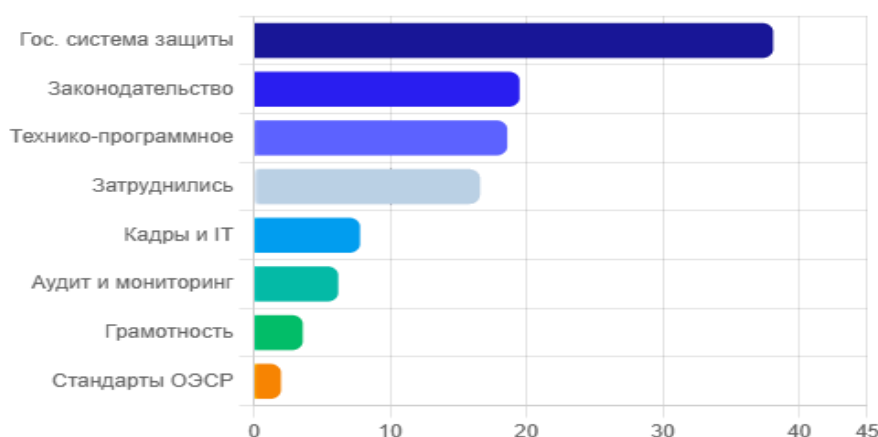


Рисунок 4. Распределение кластеров общественного запроса (%)

По результатам анализа 307 ответов респондентов на открытый вопрос: «Какие меры государство должно принять, чтобы защитить данные налогоплательщиков от киберугрозы?», и выявлены 8 основных содержательных тем.

1. Усиление общей кибербезопасности и комплексной защиты данных — 117 человек (38,1%). Наибольшая доля респондентов подчеркнула необходимость построения надежной государственной системы защиты, систематического ограничения доступа к конфиденциальным базам данных, а также усиления мер безопасности межведомственной системы электронного взаимодействия «Түндүк».

2. Ужесточение законодательства и повышение правовой ответственности — 60 человек (19,5%). Около пятой части опрошенных считают ключевым фактором введение строгой уголовной и административной (штрафной) ответственности за утечку и незаконное разглашение персональных данных, принятие профильных законодательных актов и усиление контроля со стороны правоохранительных органов.

3. Совершенствование технической и программной защиты — 57 человек (18,6%). Респонденты отметили важность реализации конкретных технических решений: внедрения многофакторной аутентификации (МФА), тотального шифрования данных, регулярной смены паролей и кодов доступа, а также своевременного обновления серверов и специализированного программного обеспечения.

4. Затруднившиеся с ответом или не имеющие конкретного мнения — 51 человек (16,6%). Данную группу составили респонденты, давшие неопределенные или краткие ответы формата: «Не знаю», «Затрудняюсь ответить» или «Билбейм».

5. Привлечение квалифицированных IT-специалистов и подготовка кадров — 24 человека (7,8%). Участники опроса указали на необходимость привлечения опытных программистов и экспертов по кибербезопасности в государственный сектор, что требует повышения уровня заработной платы и создания благоприятных условий труда для квалифицированных IT-кадров.

6. Регулярный мониторинг, аудит систем и проверка на уязвимости — 19 человек (6,2%) Респонденты акцентировали внимание на важности непрерывного кибермониторинга: систематической проверки баз данных на наличие уязвимостей («брешей»), проведения независимого IT-аудита и формирования механизмов оперативного реагирования на инциденты и кибератаки.

7. Повышение цифровой и киберграмотности — 11 человек (3,6%). Отмечается необходимость проведения обучающих программ, тренингов и информационных кампаний как для налогоплательщиков, так и для сотрудников налоговых органов по вопросам базовой информационной безопасности и защиты от фишинговых атак.

8. Использование международного опыта и глобальных стандартов — 6 человек (2,0%) Наименьшая доля опрошенных указала на целесообразность изучения лучшей мировой практики и внедрения международно признанных стандартов кибербезопасности (в частности, рекомендаций ОЭСР / OECD).

На основе проведенного анализа сформулированы следующие ключевые выводы и рекомендации для органов государственной власти Кыргызской Республики.

Прямая угроза сжатию налогооблагаемой базы. Риск утечки данных перестает быть изолированной IT-проблемой и становится фактором прямого экономического ущерба. Риск компрометации фискальной информации 75,5% респондентов оценивают как критический параметр, способный мотивировать их к уходу в теневую экономику или прекращению деятельности. Вложения в кибербезопасность ГНС следует квалифицировать не как текущие административные издержки бюджета, а как высокорентабельные инвестиции в сохранение налогооблагаемой базы.

Парадокс институционального доверия и системы «Тундук». Принудительная интеграция бизнеса в цифровые сервисы без предоставления юридических гарантий защищенности формирует латентное сопротивление реформам. Государству необходимо сместить акцент с принуждения на формирование прозрачной системы аудита безопасности данных.

Совершенствование нормативно-правовой базы. Необходима имплементация норм об адресной уголовной и финансовой ответственности должностных лиц за компрометацию данных ГНС. Законодательство должно предусматривать прозрачные механизмы финансовой компенсации прямых и косвенных убытков бизнеса, возникших в результате утечек.

Защита внешнеэкономического контура (ВЭД). При участии в интеграционных процессах ЕАЭС и соглашениях автоматического обмена информацией (CRS/AEOI) Правительству КР следует настаивать на применении единых протоколов сквозного шифрования и взаимного аудита, исключающих риски промышленного шпионажа и раскрытия коммерческой тайны отечественных экспортеров перед иностранными конкурентами.

Независимый IT-аудит и кадровое переформатирование. Достижение доверия невозможно без регулярного кибераудита систем ГНС с привлечением независимых международных сертифицирующих органов (стандарты ISO/IEC 27001). Кроме того,

необходимо пересмотреть уровень оплаты труда квалифицированных IT-специалистов в государственном секторе для предотвращения утечки кадров в частный сектор и за рубеж.

Список литературы:

1. Acemoglu D., Robinson J. A. Why Nations Fail: The Origins of Power, Prosperity, and Poverty. New York: Crown Business, 2012. 544 p.
2. Levi M. Of Rule and Revenue. Berkeley: University of California Press, 1988. 253 p.
3. Gordon L. A., Loeb M. P. The Economics of Information Security Investment // ACM Transactions on Information and System Security. 2002. V. 5. №4. P. 438–457.
4. OECD. Standard for Automatic Exchange of Financial Account Information in Tax Matters, Second Edition. Paris: OECD Publishing, 2017. 320 p.

References:

1. Acemoglu, D., & Robinson, J. A. (2012). Why Nations Fail: The Origins of Power, Prosperity, and Poverty. New York.
2. Levi, M. (1988). Of Rule and Revenue. Berkeley.
3. Gordon, L. A., & Loeb, M. P. (2002). The Economics of Information Security Investment. *ACM Transactions on Information and System Security*, 5(4), 438–457.
4. OECD (2017). Standard for Automatic Exchange of Financial Account Information in Tax Matters, Second Edition. Paris.

Поступила в редакцию
20.08.2026 г.

Принята к публикации
29.08.2026 г.

Ссылка для цитирования:

Эргешова А. Р., Орозмаматова Д. А. Информационная безопасность в сфере налогового администрирования: эмпирический анализ общественного восприятия и институционального доверия в Кыргызской Республике // Бюллетень науки и практики. 2026. Т. 12. №10. С. 448-454. <https://doi.org/10.33619/2414-2948/131/49>

Cite as (APA):

Ergeshova, A., & Orozmatova, D. (2026). Information Security in Tax Administration: an Empirical Analysis of Public Perception and Institutional Trust in the Kyrgyz Republic. *Bulletin of Science and Practice*, 12(10), 448-454. (in Russian). <https://doi.org/10.33619/2414-2948/131/49>